CHAPTER

10

ORGANIZING NETWORK RESOURCES

After reading this chapter and completing the exercises, you will be able to:

- Understand the differences between an Active Directory domain and a Windows NT domain
- Explore Active Directory organizational units, domains, trees, and forests
- Maintain and control the Active Directory
- Understand how Active Directory maintains its files and logs
- Complete a backup of the Active Directory
- Recover and restore the Active Directory in case of failure

A major drawback of Windows NT was its flat directory structure. In the Windows NT networking world, there were really only two types of users: administrators and regular users. Administrators were all-powerful, whereas regular users really had no permissions to handle any management functions. In small organizations with one or two administrators, this structure was not really an issue because administrators could easily communicate any changes that they wanted to perform on the network. In large enterprise environments with many administrators, however, different levels of administrators are needed. For example, there might be a need for an administrator to control all users and groups in a specific department without that administrator having the power to modify users and groups in any other department. The only way to accomplish this task in Windows NT was to create multiple domains, which is not the most efficient way of designing a Microsoft Windows NT network.

With Windows 2000, Microsoft introduces a new way of looking at directory objects, such as users and groups. This new method is known as the Microsoft **Active Directory**. With Active Directory, Windows 2000 offers a way to create users with different permissions. Instead of giving a user the permission to modify all users and groups (as is the case in Windows NT), Windows 2000 allows you to give them the permission to modify only certain users and groups.

This chapter discusses the Microsoft Active Directory, and how you should prepare, design, maintain, and recover it. You will also learn the differences between a Windows NT domain and a Windows 2000 Active Directory domain.

User and Resource Identification

Before you can truly understand what Active Directory means for your organization, you need to be clear on the differences between an Active Directory domain and a Windows NT domain. The best way to understand these differences is to compare the logical structures of the two types of domains. In the following sections, you will learn the components that make up both of these directories.

Active Directory consists of as many as five components:

- Object
- Organizational unit
- Domain
- Tree
- Forest

The subsequent sections detail each of these components and describe how they fit into the Active Directory scheme.

Object

An **object** is the smallest unit within the Active Directory. The role of the Active Directory is to control all of these objects. Objects can include computers, contacts, groups, printers, shared folders, and users.

Objects can be further divided into their **object attributes**. The object attributes define the configuration of each object. For example, a user object can contain several attributes, including first name, middle initial, last name, logon name, password, and description. Some of these attributes are mandatory, such as a name (either the first name, last name, or initials) and a logon name (see Figure 10-1). Other attributes are optional, such as a password and description.

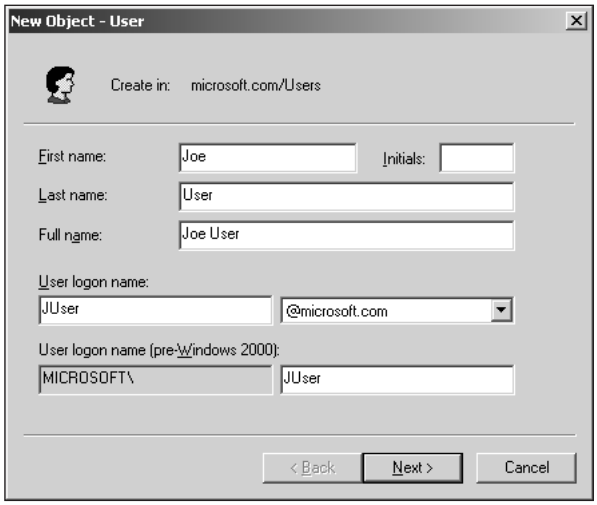

Figure 10-1 Active Directory object attributes

Microsoft has designed Active Directory so that you can extend it and modify it as you see fit. To do so, you need to create definitions for new objects, or **object classes**. The definitions for all object classes within the Active Directory are stored within the **schema**. The schema is the way in which the Active Directory recognizes different objects. You can modify the schema to add information, such as a user's picture.

Organizational Unit

An **organizational unit (OU)** is a container that organizes objects within a domain into a single administrative unit. You can then assign permissions or administrative roles to these organizational units. Organizational units can also be used to separate departments (such as Accounting, Research and Development, and Human Resources) and maintain all of their resources in one place. For example, you may want to configure an Accounting OU to contain all users, groups, computers, and printers that belong to the Accounting department. A single administrator could then be assigned to this OU who would manage this OU and no others. Figure 10-2 shows an example of an organizational unit. In the figure, the Human Resource OU contains a document that can be sent to the printer located in the Accounting OU.

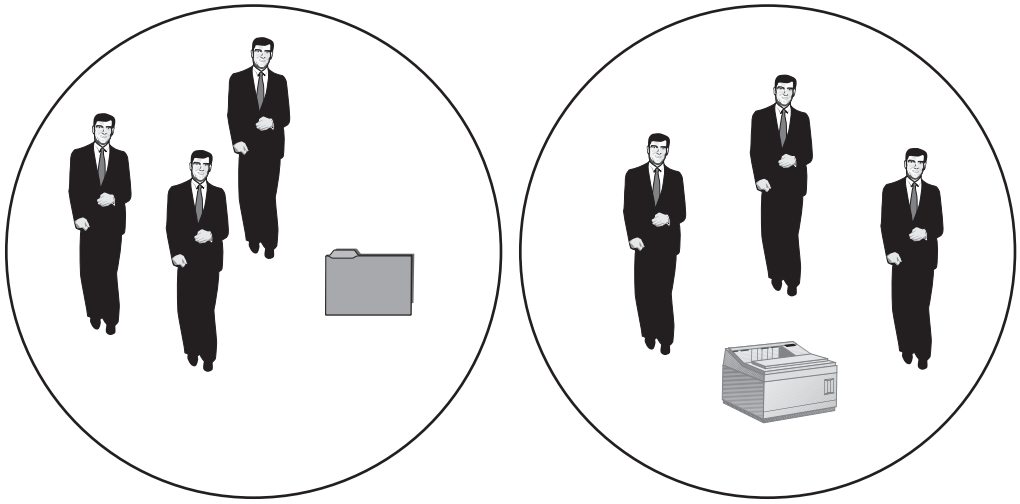

Figure 10-2 Organizational unit

Domain

It is important to understand the differences between a Windows 2000 Active Directory domain and a Windows NT 4.0 domain. In essence, an **Active Directory domain** is the same as an Internet domain, whereas a **Windows NT domain** is a logical collection of computers that share the same security information and user database.

A domain is a security context that is assigned to multiple computers and users. Domains are logical, meaning that computers in the domain do not need to be physically close to one another. In fact, two computers connected to the same Ethernet hub may reside in different domains. Each will have the security set to it by the domain controllers. All objects within a domain share the same administration configuration, security context, and directory replication.

A Windows 2000 domain differs from a Windows NT domain in the way in which the domain controllers are configured and maintained. First, you will learn how Windows NT domains operate. You will then find a definition of how Windows 2000 domains differ.

In Windows NT, a single domain will have a single **primary domain controller (PDC)** and, optionally, one or more **backup domain controllers (BDCs)**. The PDC maintains the only version of the directory database that can be directly updated. All changes to the database are performed on the PDC and then replicated to the BDCs. If the PDC goes offline, no changes to the domain may be made, including modification of user properties or computer memberships in the domain, until a BDC is promoted to become a PDC.

During this promotion stage, information that has not been replicated from the PDC to the BDC may be lost.

Windows 2000 uses the **multimaster replication** method. With this method, each **domain controller** stores and maintains a writable, or read-write, version of the portion of the Active Directory database that belongs to its domain, or its domain's partition. When any changes are made to the databases of any of the domain controllers, they are replicated to all members of that domain. Because all domain controllers maintain the same read-write Active Directory database, the entire Active Directory partition is available to any domain controller at any time. If a domain controller fails, the other domain controllers within the domain will automatically take over its role until it comes back into the network. Figure 10-3 depicts an Active Directory domain.

The read-write portion of the Active Directory database is also known as a **replica**.

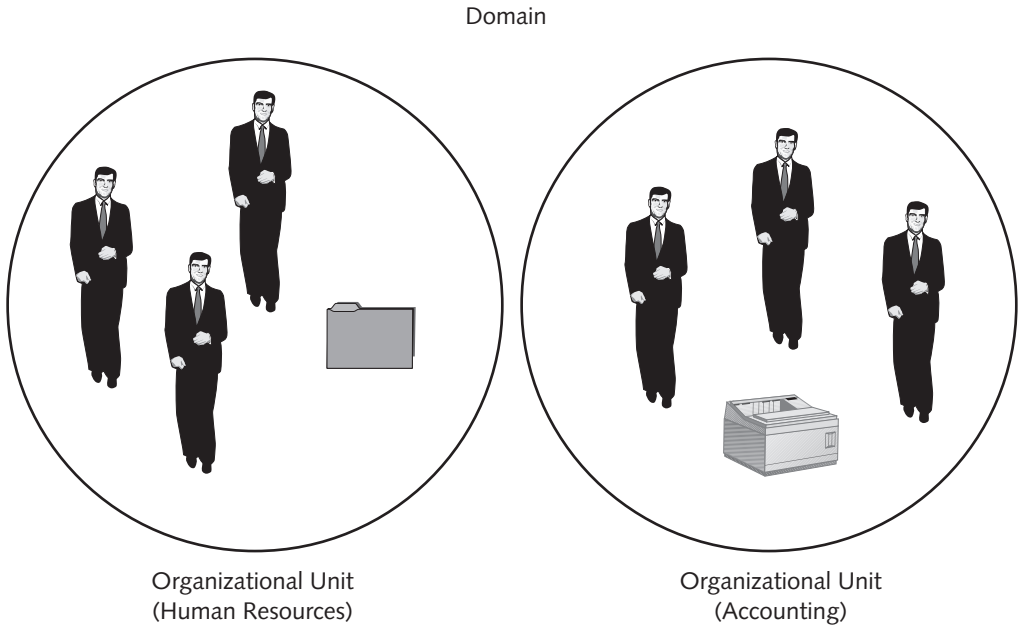

Figure 10-3 Active Directory domain

Tree

When multiple domains are connected so that they share a common schema, a **tree** is created. Domains within a tree are linked together by using **trust relationships**. Unlike with Windows NT, Windows 2000 trust relationships are based on the Kerberos protocol. Previously, trust relationships were not secured by a protocol.

Unlike in Windows NT, trust relationships are transitive in Windows 2000. That is, if you have three domains in your organization (Accounting, Human Resources, and R&D), and Accounting trusts Human Resources and Human Resources trusts R&D, then Accounting will automatically trust R&D.

All domains within a tree share a common root domain name (for example, Lanw.com). Figure 10-4 shows an example of a Windows 2000 tree.

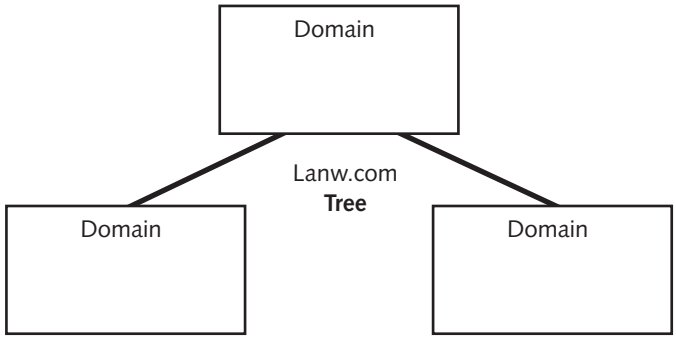

Figure 10-4 Active Directory tree

Forest

When one or more trees do not share the same root domain name but maintain the same schema and configuration, they are said to be part of a **forest** (see Figure 10-5). All trees within the forest trust each other using automatic transitive trusts. If your organization has multiple forests in it, explicit trusts must be configured.

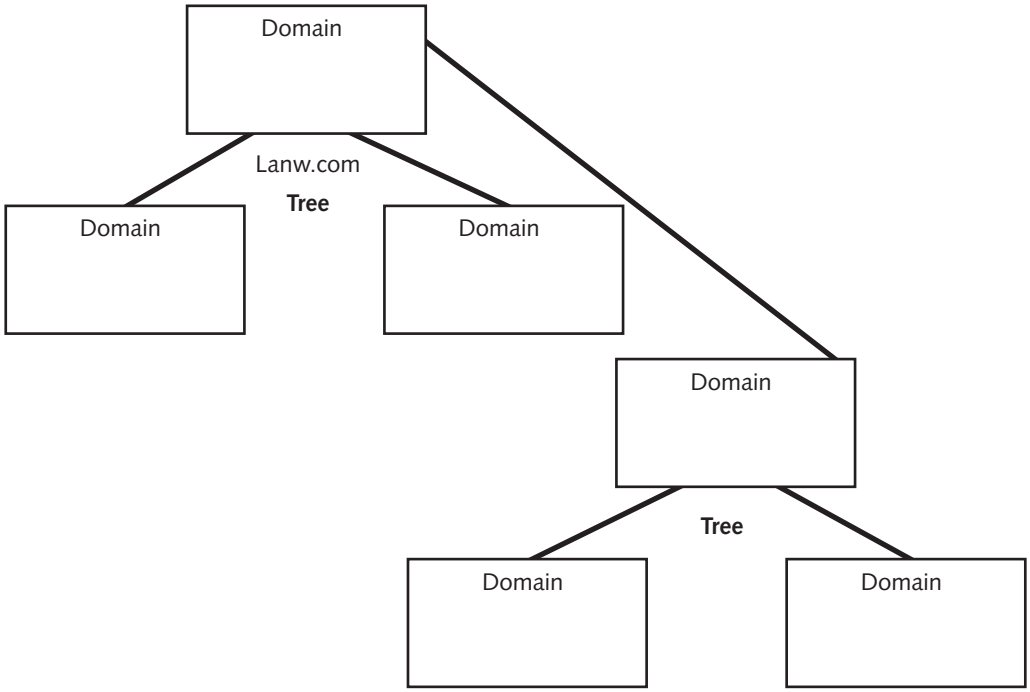

Figure 10-5 Active Directory forest

PREPARING FOR ACTIVE DIRECTORY

Microsoft's Active Directory is an extremely complex system. Although you may not fully understand all of its inner workings, you must be aware of how to prepare for Active Directory. Two scenarios for installing Windows 2000 with Active Directory exist: upgrading an existing Windows NT network and installing a new Windows 2000 network. The next two sections will detail some of the prerequisites and criteria that must be met before installing Active Directory.

Upgrading an Existing Windows NT Network

Remember that Windows 2000 Active Directory is based on the Internet domain structure and therefore requires you to install and configure TCP/IP and DNS. Active Directory installation is covered in Hands-on Project 10-1.

When your organization decides to upgrade its existing network to a Windows 2000 network, you may have to deal with some basic issues. Windows 2000 can run in one of two modes: **mixed mode** or **native mode**. Any time that at least one domain controller is still running Windows NT, the network is said to be running in mixed mode.

Mixed Mode

Mixed mode is necessary because of the way in which Windows NT and Windows 2000 differ. In a Windows NT network (one that is configured with domains), a single domain controller acts as the PDC. That system maintains the directory database and is the only system that can modify this database. In a Windows 2000 network, every domain controller maintains a read-write copy of the database. Modifications take place on the local domain controller, with the updated information being replicated to all of the members within the domain. If you were to configure a network with both Windows NT and Windows 2000 domain controllers, you would have an obvious problem: The Windows 2000 domain controllers would attempt to modify the database on their own, without notifying the PDC.

To support the Windows NT networking model, each Windows 2000 domain can designate a single domain controller to act as a PDC. This domain controller is known as the **PDC emulator**. It is the first domain controller that is upgraded in the Active Directory domain that assumes this role. As far as the Windows NT BDCs are concerned, this domain controller becomes the PDC and therefore controls all changes to the domain. Any new Windows 2000 domain controller that is added will maintain a read-write copy of the database (as per the Windows 2000 multimaster replication model). It then simply acts as a gateway between the Windows 2000 and the Windows NT networks. Because the Windows 2000 PDC emulator appears to be a Windows NT PDC to the rest of the Windows NT network, no changes need to be made on the clients. They will still see the network as though nothing has changed.

Once all domain controllers in the domain have been upgraded to Windows 2000, the network will continue to run in mixed mode. To change the way in which the network operates, you would have to manually reconfigure the network into native mode.

Native Mode

As the name implies, native mode is the way in which Windows 2000 systems communicate with other Windows 2000 systems. For this mode to work, you need to upgrade all of your domain controllers to Windows 2000. Table 10-1 highlights the differences between a Windows 2000 network running in mixed mode and one that is running in native mode.

Table 10-1 Mixed mode versus native mode

Mixed Mode	Native Mode
Multimaster replication	Multimaster replication
Nontransitive trusts	Transitive trusts
Only global and local groups exist because Windows NT does not support other group types	All Windows 2000 groups are supported, including domain local, local, global, and universal
No nested security groups	Nested security groups

The easiest way to upgrade an existing Windows NT network to Windows 2000 is to perform an **in-place upgrade**.

In this type of upgrade, all current domain configurations are maintained. Before you complete an upgrade, however, Microsoft recommends that you perform the following steps:

- Back up your current system, especially the domain controllers.
- Verify that the backups were completed and the data on the tapes are valid.
- Synchronize the entire domain. This step ensures that all domain controllers have the most up-to-date information.
- Remove one BDC from the network. This BDC will be used for two tasks. First, it will be used to check the backup of the domain. Second, it will be maintained as a backup during and after the upgrade (for one or two weeks). Once this BDC is removed from the domain, promote it to a PDC and make sure that no directory data have been corrupted. Restore the backup and again verify that no directory data have been corrupted.

Once you have tested the backup for the Windows NT domain, you can upgrade the PDC to Windows 2000. Once the upgrade is complete and stable, you can upgrade each of the remaining BDCs.

Installing a New Windows 2000 Network

The simplest way to install Windows 2000 Active Directory is by installing a fresh copy of the operating system on all servers. This tactic may not be feasible for most organizations, but it is the cleanest way to install the system. One problem with such an installation is that all users, groups, and applications must be reinstalled on the domain.

When installing Active Directory on a Windows 2000 Server, you use the Active Directory Installation Wizard. This wizard introduces a new feature into Windows 2000 that has been lacking from the Windows NT networking world since its initial release: the ability to upgrade and downgrade regular servers to domain controllers. In Windows NT, you had the option to configure the server as either a PDC, a BDC, or a stand-alone server. Once this choice was made, the only way to make a domain controller become a stand-alone server or a stand-alone server become a domain controller was to reinstall the operating system. Today, third-party tools and nonsupported methods of moving a domain controller from one domain to another are available, but there is no way to install or uninstall the domain controller components. The Active Directory Installation Wizard (see Figure 10-6), called **Dcpromo.exe**, is found in the WINNT\System32 directory. It allows you to install your server as a domain controller or to remove it as one. Note that doing so requires you to reboot the server.

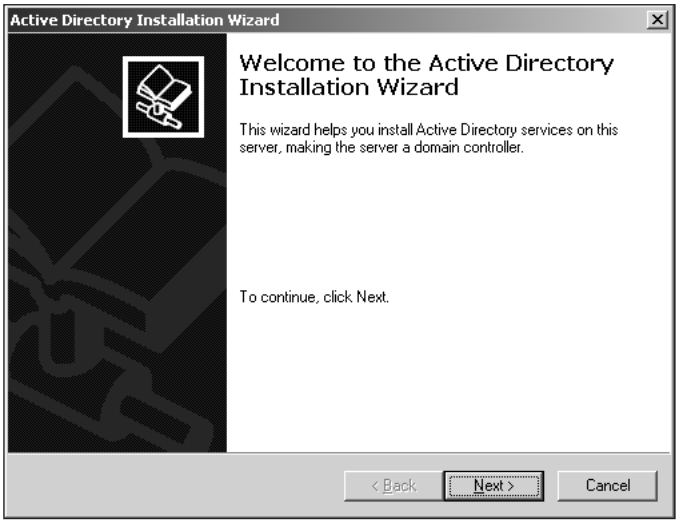

Figure 10-6 Active Directory Installation Wizard

When running the Active Directory Installation Wizard, your server must have an NTFS partition that is formatted in NTFS version 5. The installation will fail if no such partition exists.

The installation wizard gives you the choice either to configure DNS yourself or to have the wizard do it for you.

Remember that Windows 2000 depends on TCP/IP and especially on DNS. Without DNS, Active Directory will not function properly. If your organization has registered its Internet domain with an Internet registrar (such as Network Systems), then you can use that domain name for the Active Directory domain name (for example, sprockets.com).

Designing Directory Structures

No set rules dictate how you must design and name your Active Directory structure. Every organization will take a different tack. These differences could reflect the inherent way in which the organization is structured (a small local organization versus a large, multinational one). Nevertheless, one configuration item must exist and must follow a set of rules: the root domain.

The first domain that you install and configure in Active Directory is known as the **root domain**. When you choose a root domain, you must follow certain guidelines:

- Choose a name that will not change. Although some name changes are unavoidable, such as those caused by a corporate restructuring or a merger, you should nevertheless try to stick with a name that is static.
- Make sure that the name matches your organization's Internet name. This choice will ensure connectivity between Active Directory and the Internet. For example, everyone knows that Microsoft's domain is *microsoft.com*.

The levels within the Active Directory tree will depend on the organization in which Active Directory is being installed. Some organizations will choose to name the child and grandchild domains based on geographical locations, whereas others will use department names (for example, *seattle.microsoft.com* and *sales.microsoft.com*). It does not matter which method your organization decides to use—just make sure to adhere to this standard. Nothing is more confusing than a domain that uses both of these methods at the same level. (For example, using both at the same time would introduce the question for Microsoft: Where is the sales team in relation to the Seattle office? Or, is there no sales department in Seattle?) You can, however, use both methods effectively, such as in the following example:

sales.seattle.microsoft.com and *sales.newyork.microsoft.com*.

Once your organization has determined its preferred domain structure, you can start to design the organizational unit structure. Remember that OUs are containers used to collect information about objects and to set properties about them, such as applications, computers, groups, policies, printers, shares, and users.

One of the main strengths of creating and implementing organizational units is that they permit delegation of administration. A new feature in Windows 2000, **delegation of administration** allows you to implement users having different permissions. For example, you can create a marketing organization unit and assign an administrator to it. That administrator will have the right to modify the objects within the marketing organizational unit, but not in organizational units that exist above it.

Troubleshooting Active Directory

Before you can successfully troubleshoot and recover your network's Active Directory, you should understand how the Windows 2000 Active Directory stores data. The following sections will look at the files that are used to store the Active Directory database information, then examine the backup and recovery of that data.

Active Directory uses a transaction-based system for storing its information. The Active Directory is descended from the Microsoft Exchange Directory. In fact, Microsoft used some of the developers of the Exchange Directory to develop the Active Directory for Windows 2000. All modifications to the Active Directory database are carried out as transactions. This method allows for the design of highly recoverable databases. If some of the data becomes corrupted, Active Directory can rebuild the lost data from the transaction log files.

The following four steps follow the process involved in modifying the Active Directory:

1. An administrator makes a change to the Active Directory, such as modifying a group membership, and Active Directory creates a corresponding transaction.
2. The transaction is written to a log file on the disk.
3. The transaction is committed to the Active Directory database stored in memory.
4. The transaction is written to the database stored on disk. This task is normally completed at shutdown and at system idle times.

Active Directory Files

The Active Directory files can be separated into two categories: the database file and the log files. The database file stores all of the Active Directory information, whereas the log files store the transactions before they are committed to the database and maintain these transactions. The following log files exist in Active Directory:

- Transaction log files
- Checkpoint file
- Reserved log files

Database File

The database file is stored in the WINNT\NTDS directory (see Figure 10-7) and is called Ntds.dit. This file stores all Active Directory components (such as users and groups), the relationships between objects (these users are members of these groups), and the schema information (the objects that exist within the Active Directory).

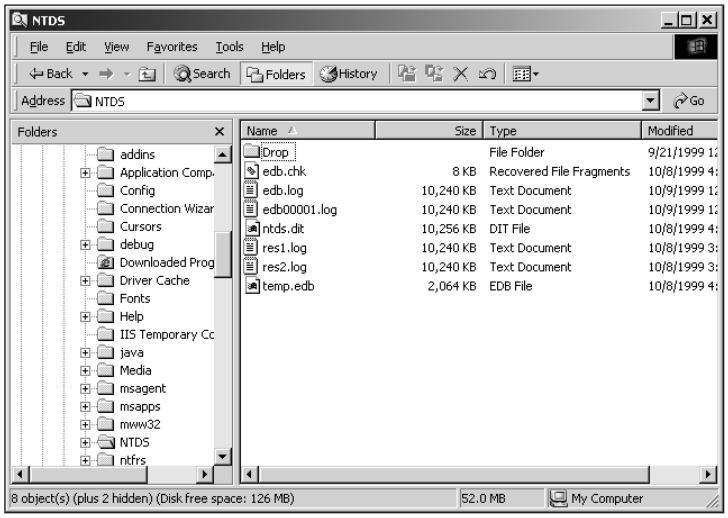

Figure 10-7 The Active Directory database and log files

Transaction Log Files

The transaction log files store all of the transactions before they are committed to the database. Notice that there is usually more than one log file and that each log file is approximately 10 MB in size. The current log file is called Edb.log. The log files are automatically set to 10 MB by the Active Directory as a placeholder, even if they contain little or no information. Once a log file is filled, it is renamed using the following naming convention:

EDBxxxxx.log

These log files are deleted when a backup is completed, as you will see in the next section. Microsoft Active Directory can log transactions in one of two ways:

- Circular logging disabled
- Circular logging enabled

With **circular logging**, the older log files are overwritten when the current log file is filled to capacity. When this option is enabled, data recovery is greatly minimized, because not all transactions may be available during the recovery process. By default, circular logging is disabled.

Checkpoint File

The checkpoint file (Edb.chk) is simply a pointer to the committed transactions. Once transactions are committed to the database, the checkpoint file is modified to reflect the noncommitted transactions. This process ensures that transactions are committed in sequence and only once.

Reserved Log Files

Active Directory automatically creates reserved log files (Res1.log and Res2.log). These log files are 10 MB in size and serve as an emergency storage location. When the transaction log file is full and Active Directory attempts to create a new one, if no more disk space exists, the transactions will be written to these two reserved log files. In this event, Active Directory will shut itself down and report an out-of-disk-space error in the event log.

Backing Up the Active Directory

Luckily for Windows 2000 administrators, the Windows 2000 new backup utility is aware of the Active Directory and will back it up properly. When you back up your system, you will notice that a new entry exists that you can select, called **System State**. Within the System State, you can choose which components to back up, such as the Active Directory, the boot files, and the Registry (see Figure 10-8). When this option is selected, all Active Directory information will be backed up.

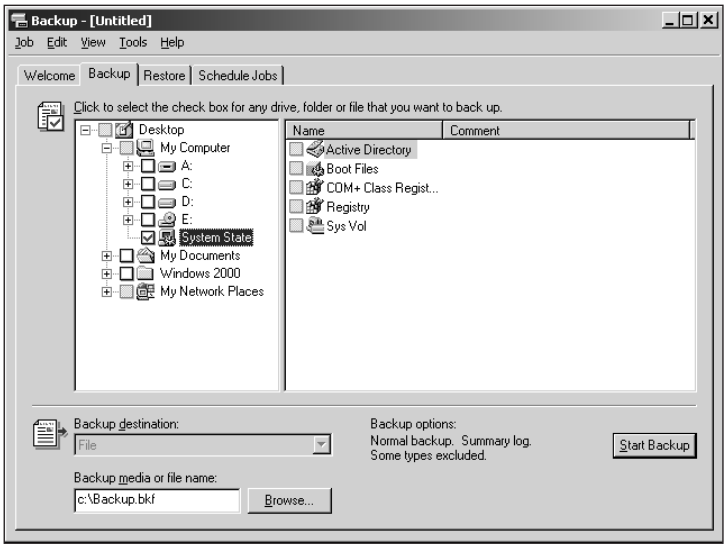

Figure 10-8 Backing up the System State

Recovering and Restoring the Active Directory

Recovering the Active Directory is somewhat more complex, because Windows 2000 will not let you restore the Active Directory while the service is running. To complete a recovery, you must reboot your server and choose the Directory Services Restore Mode option (see Hands-on Project 10-6). Once the system is restarted using this method, you can choose the System State\Active Directory option from the Restore tab of the backup program. This choice will restore your Active Directory database. You would then need to restart the system to restart the Active Directory.

CHAPTER SUMMARY

- Windows 2000 introduces a new way of organizing directory objects, called the Active Directory, which provides a way to create users with only the permissions they need.
- This chapter explored the Microsoft Active Directory and showed you how to prepare, design, maintain, and recover the Active Directory.
- It also discussed the differences between a Windows NT domain and Windows 2000 Active Directory domains.
- Finally, it explored how to back up and restore Active Directory.

KEY TERMS

Active Directory — A hierarchical directory database used in Windows 2000 to store all object information, including information about users, groups, and computers.

Active Directory domain — A logical domain of Windows 2000 computers that share the same security and user information.

backup domain controller (BDC) — A Windows NT Server that maintains a read-only version of the directory database to authenticate users.

circular logging — A process by which older log files are overwritten as the current log file fills to capacity. When this option is enabled, data recovery is greatly minimized.

Dcpromo.exe — The Active Directory Installation Wizard, which is found in the WINNT\System32 directory. This wizard allows you to install your server as a domain controller or to remove it as one.

delegation of administration — A Windows 2000 feature that allows you to implement users having different permissions. For example, you can create an organizational unit and assign an administrator who will have the right to modify the objects within that organizational unit, but not in organizational units that exist above it.

domain controller — A Windows 2000 Server that authenticates users in a Windows 2000 network.

forest — A collection of two or more trees with noncontiguous namespace.

in-place upgrade — An upgrade to Windows 2000 in which all current domain configurations are maintained.

mixed mode — A mode in which Windows 2000 runs so as to maintain backward compatibility with Windows NT domains.

multimaster replication — A situation in which all domain controllers maintain a read-write copy of the database that they replicate to all other domain controllers.

native mode — The way in which Windows 2000 systems communicate with other Windows 2000 systems.

object — A component of the Active Directory, such as a user, group, computer, or application.

object attributes — Configuration variables for objects.

object classes — The definitions for new objects and for object classes within the Active Directory, which are stored within the schema.

organizational unit (OU) — A way to maintain a set security model for several objects within a domain. Similar to Windows NT domains.

PDC emulator — A service that runs on a Windows 2000 system that emulates the single-master replication method used in Windows NT. This service is used until all servers have been upgraded to Windows 2000.

primary domain controller (PDC) — The Windows NT Server that maintains the master copy of the security database.

replica — A copy of part of the directory.

root domain — The top-level domain in Active Directory (for example, microsoft.com).

schema — The way in which the Active Directory recognizes different objects. You can modify the schema to add information, such as a user's picture.

System State — An option that allows you to choose which components to back up, such as the Active Directory, the boot files, and the Registry.

transitive trust — A relationship that states that if domain A trusts domain B, and domain B trusts domain C, then domain A will automatically trust domain C.

tree — A collection of domains that use the same contiguous namespace.

trust relationship — A relationship that is set up between domains so that one domain can trust resources from another domain.

Windows NT domain — A logical collection of Windows NT computers that share the same user database and security models.

REVIEW QUESTIONS

1. Active Directory is a flat database file system. True or False?
2. Windows 2000 Active Directory uses a(n) _____ replication model.
3. In a Windows 2000 network running Active Directory, every domain controller maintains a read-write version of the database. True or False?
4. Which of the following log files is used to store database transactions?
   a. Edb.log
   b. Edb00001.log
   c. Res1.log
   d. Edb.chk
5. Which of the following log files is used to store old transactions?
   a. Edb.log
   b. Edb00001.log
   c. Res1.log
   d. Edb.chk
6. Which of the following log files is used to determine which transactions have already been committed to the database?
   a. Edb.log
   b. Edb00001.log
   c. Res1.log
   d. Edb.chk

7. Which of the following log files is used in case the system runs out of disk space?
   a. Edb.log
   b. Edb00001.log
   c. Res1.log
   d. Edb.chk
8. For maximum recoverability, the log files and the database files should reside on the same partition. True or False?
9. Once a Windows 2000 Server is installed as a domain controller, it cannot be demoted to a non-domain-controller role. True or False?
10. Windows 2000 domain controllers cannot be moved from one domain to another. True or False?
11. When you want to add objects to the Active Directory Database, you would modify the _____.
12. When two or more domains share the same namespace, they are said to be in the same _____.
13. When two or more domains do not share the same namespace, they are said to be in a(n) _____.
14. Organizational units are used to group objects that require the same security rights. True or False?
15. DNS is a requirement of Active Directory. True or False?
16. Select the _____ _____ option to automatically back up certain system components, such as the Active Directory, the boot files, and the Registry.
17. With _____ _____, older log files are overwritten as the current log file fills to capacity.
18. Name the five components that make up the Active Directory.
19. What new feature in Windows 2000 allows you to implement users of different permissions?
20. What defines the configuration of each object in Windows 2000?

HANDS-ON PROJECTS

Project 10-1

To install Active Directory in a new domain:

1. Click **Start**, **Run**.
2. In the **Open** field, type **dcpromo** and then click **OK**.
3. The Active Directory Installation Wizard will appear (see Figure 10-6 earlier in the chapter). Click **Next**.

4. Choose the **Domain controller for a new domain** option, and then click **Next** (see Figure 10-9).

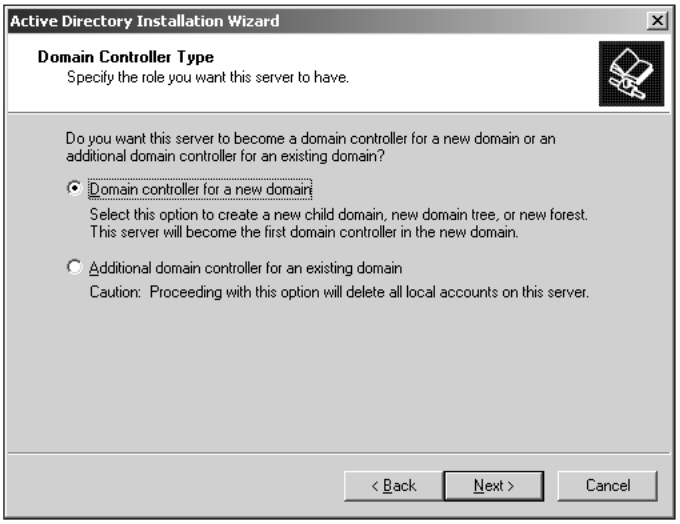

Figure 10-9 Choosing to install a new domain

5. Choose the **Create a new domain tree** option, and then click **Next** (see Figure 10-10).

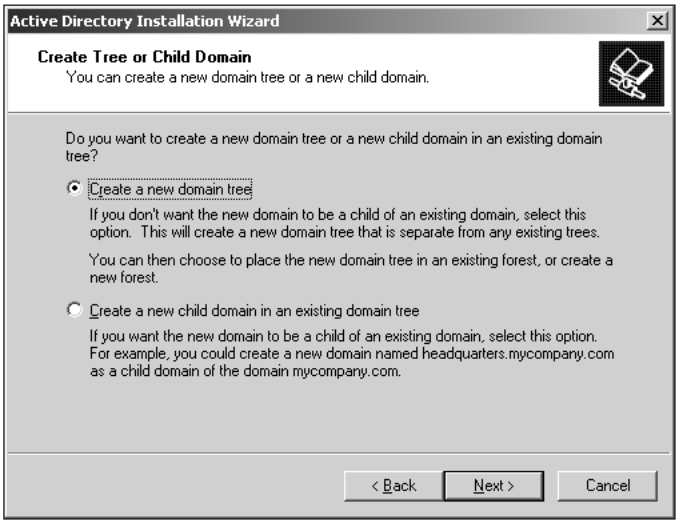

Figure 10-10 Choosing to create a new tree

6. Choose the **Create a new forest of domain trees** option, and then click **Next** (see Figure 10-11).

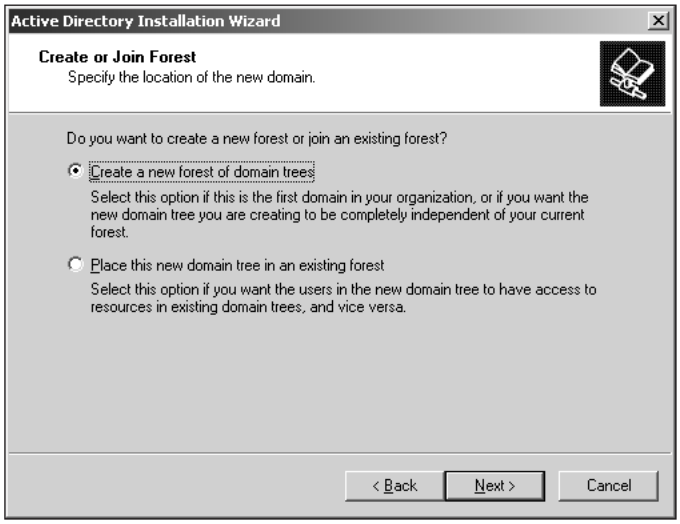

Figure 10-11 Choosing to create a new forest

7. Enter the full domain name of the desired domain, and then click **Next** (see Figure 10-12). The wizard will now check whether that domain name is already in use.

Figure 10-12 Entering the domain name

8. Enter a NetBIOS domain name for backward compatibility with Windows NT systems, and then click **Next** (see Figure 10-13).

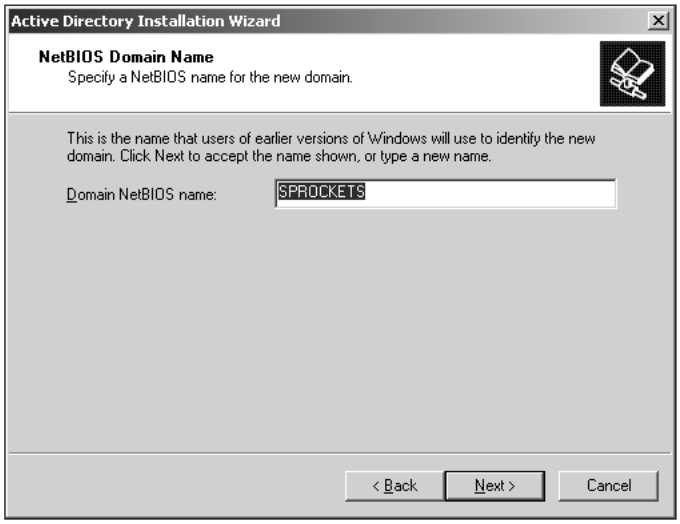

Figure 10-13 Entering the NetBIOS domain name

9. Choose a location for the Active Directory database and log files, and then click **Next** (see Figure 10-14).

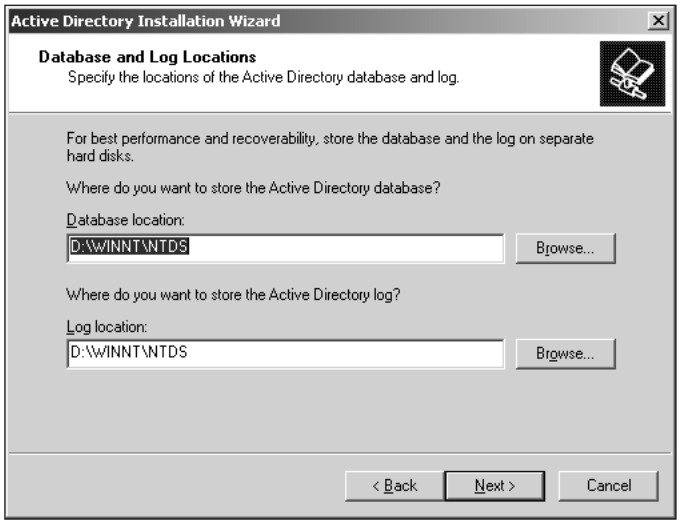

Figure 10-14 Active Directory file locations

For maximum recoverability, store the database file and the log files on two (physically different) hard drives.

10. Enter a location for the Sysvol folder (see Figure 10-15). This information will be replicated to all other domain controllers in the domain (this folder must reside on an NTFS version 5 volume).

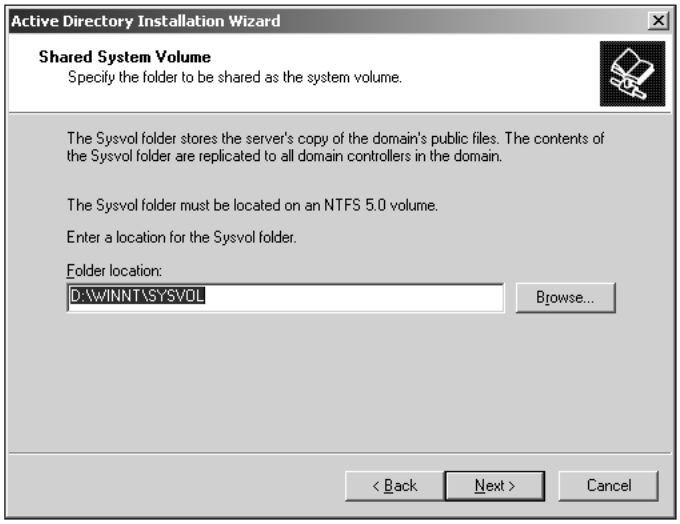

Figure 10-15 The Sysvol location

11. Choose whether to allow the wizard to automatically configure DNS for you, and then click **Next**.
12. Choose the permission compatibility for users and groups, and then click **Next**.
13. Enter a user name and password for an administrative account with the correct permissions to complete the installation, and then click **Next**.
14. Click **Next** to complete the installation. Windows 2000 will now install Active Directory.
15. Click **Finish**, and then reboot your system.

Project 10-2

To add a domain controller to an existing domain:

1. Click **Start**, **Run**.
2. In the **open** field, type **dcpromo**, and then click **OK**.

3. The Active Directory Installation Wizard will appear. Click **Next**.
4. Choose the **Additional domain controller for an existing domain** option, and then click **Next**.
5. You will be asked to authenticate the user and choose the domain.

Project 10-3

To create an organizational unit:

1. Click **Start**, **Programs**, **Administrative Tools**, **Active Directory Users and Computers**.
2. In the left pane, right-click the domain and choose **New**, **Organizational Unit**.
3. Enter a name for the organizational unit, and then click **OK** (see Figure 10-16).

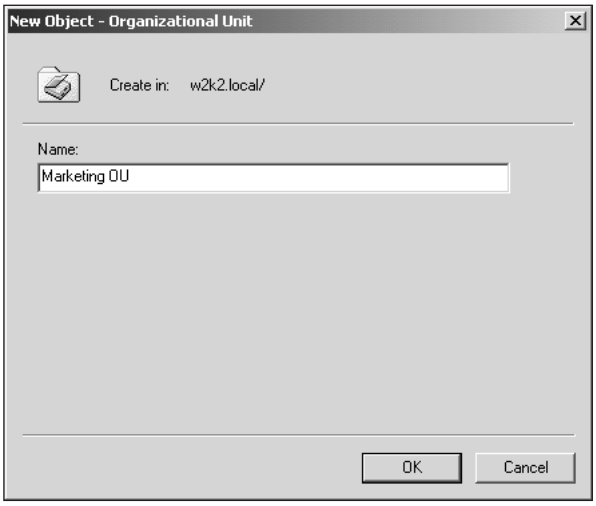

Figure 10-16 Creating a new organizational unit

Project 10-4

To enable circular logging:

1. Click **Start**, **Run**.
2. In the **open** field, type **regedt32**, and then click **OK**.
3. Browse to the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters** key (see Figure 10-17).

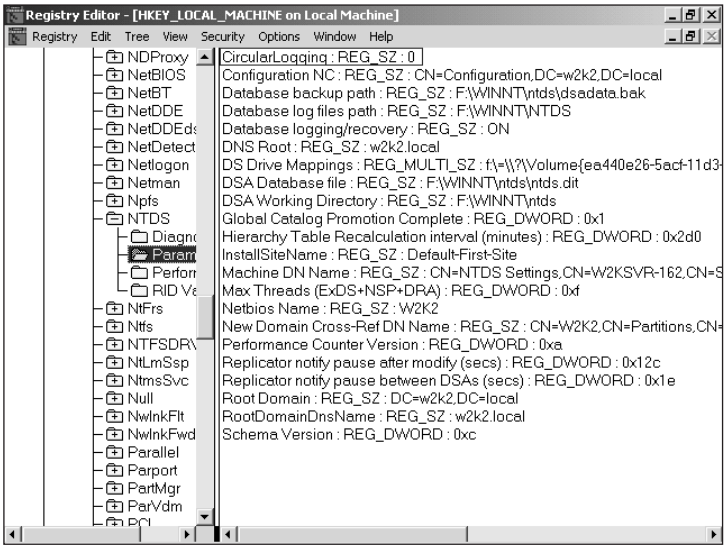

Figure 10-17 Editing the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters key in regedt32

4. To enable circular logging, select **Add Value** from the **Edit** menu and name it **CircularLogging** (See Figure 10-18). Click **OK**.

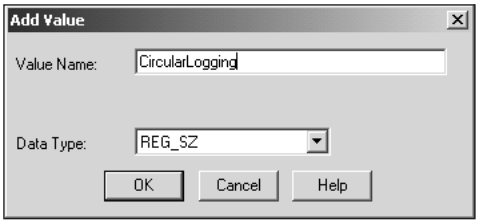

Figure 10-18 Adding a circular logging value RegEdt32

5. The String Editor dialog box appears. If you set the string to equal **1**, then circular logging will be enabled. Setting it to **0** will disable circular logging.
6. Close the Registry Editor by clicking the **Close** button at the top right of the screen.

Project 10-5

To back up Active Directory:

1. Click **Start**, **Run** and type **Ntbackup**.
2. Choose the **Backup** tab.
3. At the very least, select the **System State** option in the left pane (refer to Figure 10-8).

4. Click **Start Backup**.
5. Click **Start Backup** on the Backup Job Info dialog box.

Project 10-6

To restore Active Directory:

1. Reboot your server.
2. In the boot menu, press the **F8** key.
3. Choose the **Directory Services Restore Mode** option, and press the **Enter** key.
4. When the system restarts, log in and run the backup program.
5. Choose the **Restore** tab, select the **System State** option, and click **Start Restore**.
6. Confirm the Restore process when prompted.

CASE PROJECTS

1. Your organization is running Windows 2000 and merges with another company that is running a Windows NT domain model. How would you connect the two networks?
2. Your Active Directory server has failed. You have a good backup system, but when you run the restoration operation, it fails. Why?
3. When logging transactions, Active Directory shuts itself down and reports an out of disk space error. Why?
4. You attempt to enable your Windows NT domain controllers and Windows 2000 controllers to run in native mode, but it is not functioning properly. Why?